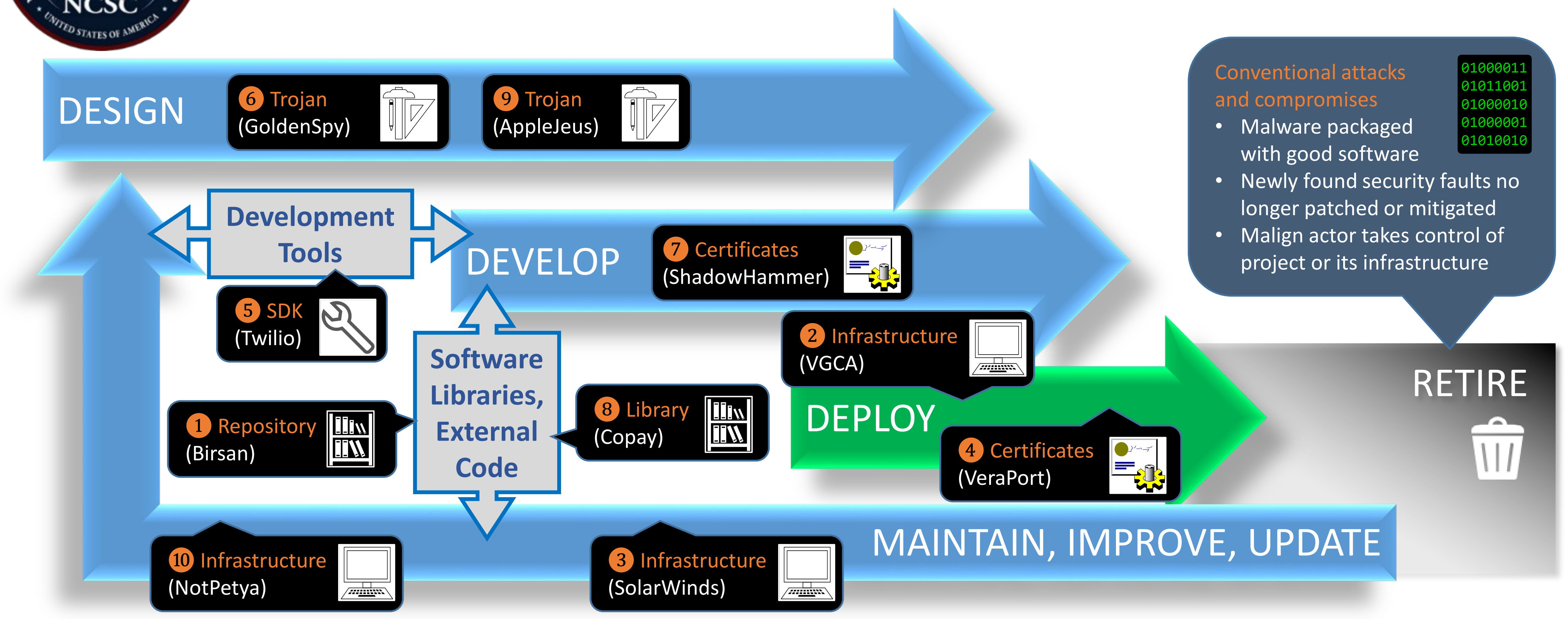
Software Supply Chain Attacks

Definition: Compromising software through cyber attacks, insider threats, or other malign activities at any stage throughout its entire lifecycle.



DESIGN

6 Trojan (GoldenSpy)

9 Trojan (AppleJeus)

Development Tools

DEVELOP

7 Certificates (ShadowHammer)

5 SDK (Twilio)

Software Libraries, External Code

1 Repository (Birsan)

8 Library (Copay)

2 Infrastructure (VGCA)

DEPLOY

4 Certificates (VeraPort)

10 Infrastructure (NotPetya)

3 Infrastructure (SolarWinds)

MAINTAIN, IMPROVE, UPDATE

RETIRE

Conventional attacks and compromises

- Malware packaged with good software
- Newly found security faults no longer patched or mitigated
- Malign actor takes control of project or its infrastructure

01000011
01011001
01000010
01000001
01010010

Software Supply Chain Attacks can target products at any stage of the development lifecycle to achieve access, conduct espionage, and enable sabotage.

- **Software supply chain attacks can use simple deception techniques such as disguising malware as legitimate products, or use complex means to access and modify the source code of genuine programs.**
- **Adversaries may seek to exploit tools, dependencies, shared libraries, and third-party code in addition to compromising the personnel and infrastructure of developers and distributors.**
- **Using software after it reaches end-of-life increases exposure to conventional cyber attacks.**

Legend	Discovered	Incident	Entry Point	Compromised Stage	Affected Software	Initial Impact	Notes
1	Feb 2021	Birsan research (Ethical hacker)	Open-Source Libraries	Development (open-source library)	Multiple	Proof-of-concept	Security researcher Alex Birsan identified improperly configured package managers at multiple major companies and verified they would install unauthorized code from public repositories instead of limiting access to internal servers.
2	Dec 2020	VGCA compromise (SignSight)	Government Certification Authority Website	Deployment (infrastructure)	Digital Signature Toolkit	Targeted government and commercial entities	Compromised a Vietnam government certificate authority and added a backdoor component to installers for legitimate software.
3	Dec 2020	SolarWinds Orion compromise	Undisclosed	Development (infrastructure)	Network Monitoring and Management Platform	Espionage	The SolarWinds Orion source code compromise represents the most significant cyber incident impacting enterprise networks across the private sector, federal, state, and local governments to date.
4	Nov 2020	VeraPort compromise	Compromised Website (Watering Hole)	Deployment (digital certificates)	Computer Utility (Browser Plugin)	Targeted government and financial websites	Targeted South Korean users of a trusted download verification tool by prompting its browser plugin to install malware signed with stolen authentic digital certificates.
5	Jul 2020	Twilio SDK compromise	Misconfigured Public Cloud Storage Bucket	Development (SDK tool)	Cloud-Based Communications	Theft	Attackers injected malicious code within the SDK library of a Communications Platform as a Service (CPAAS) company through its misconfigured cloud-hosted infrastructure.
6	Jun 2020	GoldenSpy (MITRE ID: S0493)	Over Distribution with Hidden Malicious Properties	Design (intentional)	Business Software	Targeted specific Western companies	A Chinese bank compelled Western corporate clients to install tax software containing a hidden backdoor.
7	Jan 2019	Asus compromise (ShadowHammer)	Compromised Development Infrastructure	Development (digital certificates)	Computer Utility (Software Updater)	Targeted specific individuals	Compromised manufacturer to target a pool of specific customers by delivering malware via software updates signed with authentic certificates.
8	Nov 2018	Copay compromise	Open-Source Library	Development (open-source code)	Cryptocurrency Wallet	Cryptocurrency theft	Poisoned popular open-source JavaScript library by injecting malicious code to steal cryptocurrency stored in desktop and mobile wallet software.
9	Aug 2018	AppleJeus campaign	Overt Distribution with Hidden Malicious Properties	Design (intentional)	Cryptocurrency Apps	Cryptocurrency theft	Overt distribution of software with hidden malicious properties. Persistent campaign developed and distributed innocent-looking cryptocurrency applications that contained hidden malicious content.
10	Jun 2017	NotPetya (MITRE ID: S0368)	Compromised Software Update Infrastructure	Deployment (infrastructure)	Business Software	Data destruction; disrupted commerce and services	Self-propagating data-destruction malware delivered through a software update from the developer's compromised infrastructure.

Dated: 21 March 2021

Software Supply Chain Attacks — *Adversaries Use Attack Campaigns for Access, Espionage, and Destruction*

Definition: Compromising software through cyber attacks, insider threats, or other malign activities at any stage throughout its entire lifecycle.

Adversarial Objectives

Hackers target software supply chains to gain stealthy and persistent access to secured systems and networks. These attacks enable operations ranging from the targeting of specific victims to indiscriminate attacks on connected networks.

Improved cybersecurity postures across most networks and computers have made software supply chain attack vectors increasingly attractive because many software development and distribution channels lack sufficient protections. Software supply chain attacks can be used for espionage as well as to manipulate or destroy data and provide difficult to detect access for future attacks.

Software Integrity

Software supply chain attacks are insidious because they erode consumer confidence in software providers on whom they depend for security updates. Contaminating software with malware in the development and distribution stages of the lifecycle makes it difficult to detect. In some instances, attackers have inserted malware before the software code has been compiled and signed, embedding it behind standard security signatures and decreasing the likelihood of its detection by anti-virus utilities. In other instances, attackers have injected malicious code through genuine updates and patches for software releases and upgrades.

Software Integrity Protocols

- **Code Signing:** Signed code includes a trusted, cryptographically secure indicator that verifies the software has been approved by its developer and not subsequently modified.
- **Hashing:** Developers distributing software will often provide unique strings of information generated by hashing algorithms. Users can apply the same algorithms to verify the software has not been modified**.**

…still subject to exploitation

- Malign actors can steal the cryptographic keys used to generate these security signatures, or compromise the development process before the software is completed, signed, or hashed.

Open-Source Software (OSS)

Open-Source Software (OSS) is widely available under licensing terms that ease its use, modification, and distribution of source code. Many OSS projects accept contributions and modifications from loosely affiliated, effectively anonymous programmers. Despite concerns about its vulnerabilities, OSS code remains ubiquitous and essential to computers and networks worldwide. Easy access to OSS can also expedite the discovery and remediation of vulnerabilities, however, the exponential growth of OSS projects has increased the potential attack surface and made auditing code a greater challenge. For example, the number of public repositories hosted by popular software development and source code management platform GitHub exploded from 46,000 in February 2009 to 28 million by January 2020. OSS developers would likely benefit from additional funding to audit and bug-track software that saturates nearly all aspects of the world today.

Attribution

The complexity of software supply chain attacks and the resources necessary to accomplish them often implicates state actors. Assigning culpability to specific national intelligence services, however, remains challenging.

- In July 2020, a federal grand jury indicted two hackers working with China's Ministry of State Security (MSS) for a global computer intrusion campaign targeting intellectual property and confidential business information.
- In October 2020, a federal grand jury indicted six members of Russia's military intelligence agency for cyber crimes, including the 2017 NotPetya attack which crippled banks, commerce, utilities, and logistics, causing billions of dollars in damages worldwide.
- Discovered in December 2020, the source code compromise of the SolarWinds Orion infrastructure monitoring platform is the most damaging software supply chain compromise impacting the United States to date. Although investigations are ongoing, the US Government and leading commercial cybersecurity firms have identified this Advanced Persistent Threat (APT) as likely Russian in origin.
- In February 2021, a federal grand jury indicted three North Korean computer programmers for cyber crimes that included cryptocurrency schemes supported by software supply chain attacks.

Note: Information contained herein represents the most reliable sources found in the public domain for this topic. When available, documents were used from the Department of Homeland Security CERT, FBI, recognized commercial sources, and reputable technology news outlets.

Dated: 03 March 2021